TIETOSUOJAVALTUUTETUN TOIMISTO

TUNNISTAMISTIETOJEN KÄSITTELY VÄÄRINKÄYTÖSTAPAUKSISSA

- Ohje toiminnan suunnittelemiseksi

Julkaistu 4.6.2010

www.tietosuoja.fi

Johdanto

Tämä ohje kuvaa vaiheittain, mitä tunnistamistietojen käsittelyssä, viestintäverkon tai yritys-salaisuuksien väärinkäytöstapauksien havaitsemisen tai selvittämisen tarkoituksessa, on otettava huomioon. Ohje pyrkii havainnollistamaan sähköisen viestinnän tietosuojalain (SVTSL, 516/2004) 13 a-13 k §:ien erityisiä vaatimuksia ja toimenpiteitä väärinkäytösten havaitsemiseksi ja selvittämiseksi. Ohje auttaa konkreettisten, organisaatiokohtaisten toimintamallien ja ohjeiden laadinnassa.

Ohje on jaettu kahteen eri osaan. Ensimmäinen osa on tarkoitettu tueksi tunnistamistietojen käsittelykäytäntöjen suunnitteluun tietohallintoa, turvallisuustoimintoja tai sisäistä tarkastusta ohjaaville tahoille. Suunnitteluosiossa käydään läpi toimenpidekohtaisesti 1) tietoturvatason varmistaminen 2) käyttäjien ohjeistaminen 3) tunnistamistietojen käsittelykäytäntöjen määrittely sekä 4) tiedottaminen. Ohjeen toinen osa on tarkoitettu tunnistamistietoja käytännössä käsitteleville tietohallinnon, turvallisuustoimintojen tai sisäisen tarkastuksen edustajille. Osiossa käydään läpi tietoverkon poikkeaman arviointiin liittyvät vaiheet sekä väärinkäytöksen selvittämistä seuraavat toimenpiteet. Toinen osa sisältää myös Kysymyksiä ja vastauksia – osion, jossa tunnistamistietojen käsittelyperusteita on pyritty selkeyttämään käytännön esimerkein. Käytännön esimerkeillä on erityisesti pyritty avaamaan SVTSL:n 13 §:n suhdetta SVTSL:n 20 §:n mukaiseen tunnistamistietojen käsittelyyn tietoturvatarkoituksessa.

Tämän ohjeen käyttäjän oletetaan tunnistavan olevansa sähköisen viestinnän tietosuojalain (516/2004) 2 pykälän 11 alakohdan mukainen yhteisötilaaja ja tiedostavan käsittelevänsä 8 alakohdan mukaisia tunnistamistietoja. Ohje täydentää tietosuojavaltuutetun toimiston ohjetta yhteisötilaajan oikeudesta käsitellä tunnistamistietoja väärinkäytöstapauksissa[1], jossa käydään tarkemmin läpi sähköisen viestinnän tietosuojalain 13 a-k § tunnistamistietojen käsittelyoikeutta erityisesti lainsäädännön näkökulmasta.

Väärinkäytösvalvonta ja muu tunnistamistietojen käsittely

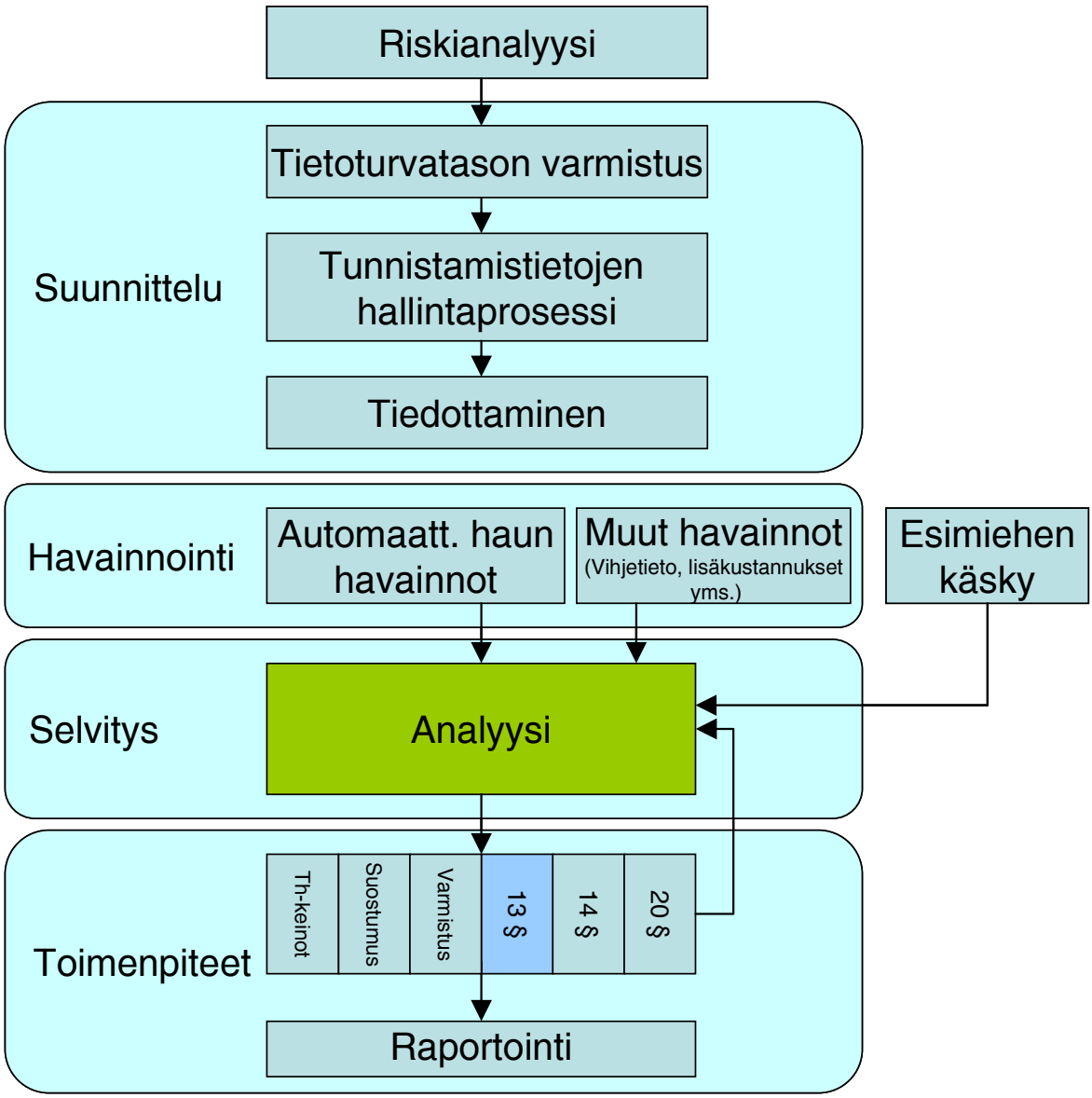
Sähköisen viestinnän tietosuojalaki sallii yhteisötilaajan toimesta tapahtuvan tunnistamistietojen käsittelyn palvelujen tuottamiseksi ja käyttämiseksi (9 §), laskutusta (10 §), markkinointia (11 §), palvelujen teknistä kehittämistä (12 §) ja tilastollista analyysia varten (12 a §) sekä väärinkäytöksien selvittämiseksi (13 §), teknisen vian tai virheen havaitsemiseksi (14 §) ja tietoturvallisuuden toteuttamiseksi (20 §).

On tärkeää tiedostaa, minkä yllä mainitun perusteen nojalla tunnistamistietoja kulloinkin käsitellään. Väärinkäytöstapauksia ajatellen erityisen tärkeää on erottaa toisistaan väärinkäytössäännösten (13 a-k §) ja tietoturvan toteuttamisperusteiden (20 §) välisen toiminnan rajat, joissa käytetyt työvälineet ja toimenpiteet ovat usein samoja, vain toiminnan päämäärän erottaessa oikeusperusteet toisistaan.

[1] Asiaa tietosuojasta 1/2009, Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa, http://www.tietosuoja.fi/46871.htm

On myös syytä erottaa viestintäverkon tunnistamistietojen käsittelyyn perustuva väärinkäytösselvitys muista tietohallinnollisista selvityskeinoista, jossa ei käsitellä tunnistamistietoja. Tietojärjestelmien sisäiset mekanismit, kuten kirjautumiset ja tietojärjestelmän käytön lokitiedot, eivät kuulu SVTSL:n 13 a-k §:ien piiriin.

Tässä ohjeessa keskitytään opastamaan viestintäverkon väärinkäytösten selvittämistä sähköisen viestinnän tietosuojalain 13 a-k §:ien mukaisella tavalla, tunnistamistietoja käsittelemällä. Ohjeessa pyritään tuomaan esiin päivittäisessä tietoverkon ylläpitotyössä esiintyvät rajanvetotilanteet väärinkäytösselvitysten ja tietoturvan huolehtimistoimenpiteiden välillä ohjeen ”Kysymyksiä ja vastauksia”-osiossa.



Kuva 1. Prosessikaavio tunnistamistietojen käsittelyoikeuksien käyttöönotosta ja käytöstä väärinkäytöstapausten selvittämiseksi

Pohjana riskianalyysi

Yhteisötilaajan päätös ryhtyä käsittelemään tunnistamistietoja väärinkäytöstapauksissa perustuu organisaation tekemään riskianalyysiin. Päätöksen teon tueksi organisaatiossa

- kartoitetaan suojattavat kohteet (keskeiset yrityssalaisuudet) ja merkittävää haittaa aiheuttavat ohjeiden vastaisen käytön tilanteet;[2]
- tunnistetaan näihin kohdistuvat riskit ja niiden vaikutukset sekä käytössä olevat hallintakeinot ja niiden riittävyys.

Organisaation johto päättää tarvitaanko tunnistamistietojen käsittelyoikeutta väärinkäytöstilanteiden havaitsemiseksi ja selvittämiseksi. Tehdyn ratkaisun mukaisesti joko käsittelyoikeuden käyttöönotto valmistellaan prosessikaaviokuvassa (kuva 1, sivu **4**) esitettyjen vaiheiden mukaisesti tai rajataan tunnistamistietojen käsittelyoikeuksia siten, ettei ko. käsittelyä tapahdu SVTSL:n 13 §:n mukaisten väärinkäytösten havaitsemiseksi ja selvittämiseksi, Käsittelytoimenpiteiden rajaamisessa suuntaa antavat viestintäviraston kannanotot ja määräykset sekä tämän ohjeen liitteenä olevat kysymykset ja vastaukset.

Apuvälineitä ja malleja

- Viestintäviraston määräykset ja päätökset http://www.ficora.fi/index/saadokset.html
- PK-yritysten riskienhallinta http://www.pk-rh.com/
- Valtionkonttorin Kaiku–Luotain: http://www.valtiokonttori.fi/public/default.aspx?nodeid=19073&contentlan=1&culture=fi-FI
- Valtionhallinnon tietoturvallisuuden johtoryhmän ohjeet http://www.vm.fi/vahti
- Kansallinen turvallisuusauditointikriteeristö KATAKRI http://www.defmin.fi/files/1525/Katakri.pdf

[2] Yrityssalaisuuksien keskeisyys määrittyy oman toiminnan, toimialan ja siellä noudatettujen käytäntöjen ja yhteistoimintamuotojen sekä käyttäjille annettujen ohjeiden kautta.
Merkittävää haittaa tai vahinkoa voi aiheutua lisääntyneistä kustannuksista tai tiedonsiirtokapasiteetin käytöstä tai muusta vastaavasta syystä, joka vaarantaa, vaikeuttaa tai hidastaa viestintäverkon tai palvelun käyttöä sille suunniteltuun käyttötarkoitukseen.

Suunnittelu

Kun organisaatio päättää ryhtyä torjumaan viestintäverkon tai -palvelun ohjeen vastaista käyttöä sekä suojaamaan yrityssalaisuuksia oikeudettomalta paljastamiselta, SVTSL 13 a-k §:ien mukaisesti omia tietoverkkojaan hyväksikäyttäen, tulee sen suunnitella ja toteuttaa tunnistamistietojen elinkaari kaikkien yksittäisten toimenpiteiden ja käsittelyvaiheiden osalta. Suunnittelu ja päätöksenteko tunnistamistietojen käsittelystä ovat johdon vastuulla, mutta mukana on hyvä olla myös henkilöstöhallinnon, tietohallinnon, viestinnän sekä lakiosaston edustajat.

Suunnittelussa tulee huomioida seuraavat lain edellyttämät ennakkotoimenpiteet:

1. Varmista tietoturvasi taso
2. Ohjeista käyttäjiä
3. Määritä tunnistamistietojen käsittelykäytännöt sekä nimeä ja kouluta tunnistamistietojen käsittelijät
4. Tiedota asiasta (käsittele YT-menettelyssä) ja tee ilmoitus tietosuojavaltuutetulle.

Tämän jälkeen yrityksellä on oikeus käsitellä tunnistamistietoja laissa säädettyjä tarkoituksia varten.

Toimenpide 1	Tietoturvatason varmistaminen
Tavoite	Tunnistamistietojen käsittely on rajattu tilanteisiin, joissa väärinkäytösten ehkäiseminen ja selvittäminen ei muuten onnistu yhteisötilaajan tietopääomansa ja tietojärjestelmiensä suojaamiseksi toteuttamien tarpeellisten tietoturvatoimenpiteiden avulla. Yhteisötilaaja on uhkien vakavuus, tekninen kehitystaso ja kustannukset huomioon ottaen pyrkinyt rajaaman tunnistamistietojen käsittelytilanteet ja käsittelyn kohteet vain ehdottomasti tarpeellisiin.
Toimenpide 1.1	Harkitse, onko pääsy viestintäverkkoon ja viestintäpalveluun ja niiden käyttöön sekä keskeisiin yrityssalaisuuksiin rajoitettu asianmukaisesti.
Toimenpide 1.2	Harkitse muiden yrityssalaisuuksien luvatonta paljastumista ehkäisevien käyttörajoituksien ja suojauskeinojen käyttöä, kuten – salassapitosopimuksien laatimista työntekijöiden ja liikekumppanien kanssa; – turvallisuusselvitysten hankkimista turvallisuusselvityksistä annetun lain mukaisesti (177/2002); – kameravalvontaa ja muuta yksityisyyden suojasta työelämässä annetun lain mukaista teknistä valvontaa; – tietojenkäsittelypalveluiden, käyttäjien ja tietojärjestelmien ryhmien eristämistä toisistaan verkoissa esim. palomuurilla tai muilla tunkeutumisenesto sovelluksilla; – pääsyn rajoittamista tiettyihin ajankohtiin sekä vain määritellyistä yhteisosoitteista tai laitteista; – siirrettävien tietojen salausta ja käytettävän salausmenetelmän määrittämistä; – liitetiedostojen tyyppien rajoittamista ja – viestien lähetyksen estämistä tietyn tyyppisiin tai tiettyihin kohdeosoitteisiin.
Toimenpide 1.3	Harkitse muiden ohjeen vastaista käyttöä ehkäisevien rajoitusten ja suojausten käyttöä, kuten – kiellettyjen kohdeosoitteiden suodatusta olemassa olevien listojen tai sisällön analyysin perusteella; – verkon ja verkkolaitteiden kuormitustilanteen seurantaa (kapasiteetin valvontaa) ja suurimpien käyttäjäryhmien asianmukaista informointia; – lähettävien ja saapuvien viestien teknistä rajoittamista (esim. viestien enimmäismäärän tai koon rajoittamista); – hyväksymättömien ohjelmien ja laitteiden asentamisen/ajamisen estämistä; – viestissä olevan ohjelmakoodin automaattisen suorittamisen es-

	tämistä; – teknisten rajoitusten kiertämisen kieltämistä.
Toimenpide 1.4	Kokoa ja säilytä sovittu aika käyttäjien toimintaa, poikkeamia, häiriöitä ja tietoturvatapahtumia koskevia tapahtumalokeja.
Esimerkkejä hyvistä käytännöistä	Toimenpiteeseen 1.1: Tietoon ja verkkopalveluihin pääsevät vain valtuutetut käyttäjät hyväksytyn pääsynvalvontapolitiikan mukaisesti. Käyttöoikeuksia hallitaan määritettyjen menettelytapojen mukaisesti.
Huomioita	Tunnistamistietojen käsittelytoimintoja ulkoistettaessa edellytetään alihankkijoilta ja yhteistyökumppaneilta vähintään samaa tietoturvatasoa kuin yhteisötilaajalta itseltään.
Apuvälineitä ja malleja	ISO 27001 ja 27002 ja valtionhallinnon tietoturvatasot.

Toimenpide 2	Käyttäjien ohjeistaminen
Tavoite	Yhteisötilaajan tietoverkon käyttäjä tietää, miten ja mihin viestintäverkkoa tai –palvelua saa käyttää ja miten epäselvissä tilanteissa tulee toimia.
Toimenpide 2.1	Dokumentoi, ylläpidä ja tuo viestintäverkon ja -palveluiden hyväksyttävän käytön säännöt kaikkien tietoverkon käyttäjien saataville. Yksilöi riittävällä tarkkuudella vähintään – viestintäverkon käytölle asetetut rajoitukset, kuten esimerkiksi se, rajoitetaanko liikennöintiä tietyn tyyppisiin tai tiettyihin kohdeosoitteisiin, – menettelyohjeet tietoaineiston käsittelystä viestintäverkossa ja – miten sääntöjen noudattamista valvotaan, miten poikkeamiin puututaan sekä mitä niiden rikkomisesta seuraa.
Esimerkkejä hyvistä käytännöistä	Käyttösäännöt käydään lävitse perehdyttämistilanteessa ja niitä käsitellään säännöllisesti järjestettävässä koulutuksessa. Niistä henkilöistä, joilla on oikeus saada tietoa keskeisistä yrityssalaisuuksista, pidetään erillistä listaa.
Huomioita	Kirjallisissa verkko- ja viestintäpalveluiden käyttöohjeissa hyväksytyn käytön tapoja voidaan määritellä laajasti, mutta tunnistamistietoja saa käsitellä SVTSL 13 a-k §:ien nojalla vain merkittävää haittaa tai vahinkoa aiheuttavien maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön tai keskeisten yrityssalaisuuksien paljastamisen havaitsemiseksi tai selvittämiseksi.

Toimenpide 3	Tunnistamistietojen käsittelykäytäntöjen määrittely
Tavoite	Väärinkäytösten hallintaohjeet on laadittu ja koulutettu.
Toimenpide 3.1	Tunnista ja määritä – ne keskeiset yrityssalaisuudet, joiden luvatonta paljastamista viestintäverkkoa tai viestintäpalvelua käyttäen organisaatio haluaa ehkäistä ja selvittää tai – ne organisaation ohjeet ja käytännöt, joiden noudattamiseksi verkon valvontaa käytetään tai on tarpeen ottaa käyttöön (ne organisaation viestintäverkon ja viestintäpalvelujen ohjeenvastaisen käytön tilanteet, jotka voivat aiheuttaa merkittävää haittaa tai vahinkoa) sekä – ne yhteisötilaajan hallinnoimat tai sen lukuun hallinnoidut viestintäverkot, joihin kertyviä tunnistamistietoja väärinkäytösten valvonnassa käytetään ja – ne yhteisötilaajan viestintäpalvelut, joita valvotaan väärinkäytösten ehkäisemiseksi tai selvittämiseksi.
Toimenpide 3.2	Nimeä tunnistamistietojen käsittelyyn selkeät vastuuhenkilöt, tehtävät tai toimintayksiköt. Näiden henkilöiden tulee olla verkon ylläpidosta, tietoturvallisuudesta tai turvallisuudesta huolehtivia tahoja.
Toimenpide 3.3	Ohjeista ja kouluta tunnistamistietojen käsittelijät asianmukaisesti.
Toimenpide 3.4	Kartoita automaattisessa viestintäverkon väärinkäytöksiin viittaavien poikkeamien haussa käytettävät järjestelmät ja määritä niissä käytettävät hakukriteerit. Hakukriteerit voivat perustua viestien kokoon, tyyppiin, yhteystapaan, liikenteen määrään tai kohdeosoitteisiin.
Toimenpide 3.5	Määritä tunnistamistietojen manuaalisen käsittelyn käytännöt väärinkäytösten selvittämistä varten.
Toimenpide 3.6	Määritä, kenelle ja millä edellytyksillä tunnistamistietoja voidaan luovuttaa. Huomaa, että tunnistamistietojen siirtäminen yhteisötilaajan ja alihankkijan välillä ei ole tietojen luovuttamista, vaan tietojenkäsittelyä yhteisötilaajan omassa toiminnassa.
Esimerkkejä hyvistä käytännöistä	Toimenpiteeseen 3.1: Määritä eri käsittelytilanteiden osalta, onko organisaatiosi viestinnän osapuoli vai viestintämahdollisuuksia järjestävä yhteisötilaaja. Toimenpiteeseen 3.2: Käytä roolikuvauksia henkilökohtaisten työnkuvien sijaan (kts. VAHTI 3/2007 liite 2: Tietoturvavastuut rooleittain). Toimenpiteeseen 3.2: Laadi näiden henkilöiden kanssa salassapitosopimukset. Toimenpiteeseen 3.2: Määritä pätevyydet, joita tunnistamistietojen

	käsittelytehtävien suorittaminen edellyttää. Toimenpiteeseen 3.3: Laadi riittävän yksityiskohtaiset menettelyohjeet tunnistamistietojen käsittelystä väärinkäytöstilanteissa. Toimenpiteeseen 3.3: Ylläpidä asianmukaiset tallenteet koulutuksesta, taidoista, kokemuksesta ja pätevyyksistä. Toimenpiteeseen 3.4: Hankkiessasi valmiita ohjelmistotuotteita väärinkäytösten valvontaan varmista, että järjestelmä mahdollistaa – määriteltyjen käsittelykäytäntöjen noudattamisen sekä – tunnistamistietoihin ja niiden käsittelyn tapahtumatietojen tarkastuspyyntöihin vastaamisen. Toimenpiteeseen 3.5: Määritä, kuka organisaatiossasi päättää väärinkäytösten selvittämisen tai muun sisäisen tutkinnan aloittamisesta. Tunnistamistietojen ottamisesta manuaalisesti käsiteltäväksi väärinkäytösten selvittämistarkoituksessa voi päättää esimerkiksi verkon ylläpidosta, tietoturvallisuudesta tai turvallisuudesta vastaava tai muu esimies. Toimenpiteeseen 3.5: Huolehdi tämän henkilön koulutuksesta väärinkäytösten selvittämiselle asetettujen edellytysten arviointiin. Toimenpiteeseen 3.5: Määritä, ketkä osallistuvat havaitun väärinkäytöksen selvittämiseen. Toimenpiteeseen 3.5: Määritä, kuka organisaatiossasi päättää toimenpiteisiin ryhtymisestä väärinkäytökseen reagoimiseksi. Toimenpiteeseen 3.5: Yhdistä tai sisällytä väärinkäytösten selvittämistarkoituksessa tehtävän tunnistamistietojen käsittelyn käytännöt sisäisen tutkinnan tai tietoturvapoikkeamiin reagoimisen toimintamalliin ja ohjeistukseen. Toimenpiteeseen 3.5: Kerätyistä tunnistamistiedoista tallennetaan tutkintakopiot tietovälineelle, jonne on pääsy vain väärinkäytöksen tutkijoilla ja heidän esimiehillään. Toimenpiteisiin 3.1 - 3.6: Ulkoistustilanteessa huolehdi yhteisötilaajana, että – ulkopuolisen palveluntuottajan kanssa on tarkasti sovittu kuka verkkoa valvoo ja missä tarkoituksessa, – ulkopuolinen palveluntoimittaja noudattaa sovittuja käytäntöjä, – tietojen siirrossa noudatettavat menettelyt on sovittu.
Huomioita	Yhteisötilaaja ei saa käsitellä omiin järjestelmiinsä kertyviä puheluihin, tekstiviesteihin tai muihin vastaaviin viesteihin liittyviä tietoja siltä osin, kun niitä välitetään kiinteissä tai matkapuhelinverkoissa. Tämä ei kuitenkaan rajoita puhelupalvelulaskun erittelytietojen käsittelyä sähköisen viestinnän tietosuojalain 24 § 2 momentin mukaisesti. Ulkoistustilanteessa yhteisötilaajan tulee varmistua ulkopuolisen palveluntarjoajan tehtävien tai toimintojen määrittelystä. Tyypillisesti verkon valvontatyökaluissa käytetyt hakukriteerit kattavat laajasti esimerkiksi erilaiset tietoturvapoikkeamat. Väärinkäytök-

	siin viittaavien poikkeamien haussa kriteerit tulee määritellä tavalla, joka rajoittaa haun vain merkittävää haittaa aiheuttavien väärinkäytöstilanteiden havaitsemiseen. Hakua ei saa käyttää lähdesuojan alaisten tietojen selville saamiseksi. Tunnistamistietojen manuaalisesta käsittelystä päättävän henkilön tulee arvioida uudelleen merkittävän haitan ja keskeisen yrityssalaisuuden edellytysten täyttyminen manuaalisen käsittelyn kohteeksi valikoituneiden tunnistamistietojen osalta. Käsittelyn kohteet ja käsiteltäväksi otettavat tunnistamistiedot tulee rajata etukäteen tapauskohtaisesti käytettävissä olevien muiden tietojen avulla. Ajallisesti käsiteltäväksi voidaan ottaa vain kulloinkin käsillä olevan tapauksen selvittämisen kannalta välttämättömät tunnistamistiedot. Tunnistamistietojen käsittely tulee päättää ja tiedot hävittää, kun käsittelyn tarkoitus päättyy esimerkiksi silloin, kun – poliisi lopettaa jutun tutkinnan, – työoikeudelliset toimenpiteet on toteutettu ja tapausta ei ole saatettu poliisitutkintaan tai – selvityksen aikana käy ilmi, että tutkinta ei ole taloudellisesti järkevää (ei ole ratkaistu tai viety poliisille tietyssä ajassa).

Toimenpide 4	**Tiedottaminen**
Tavoite	Tiedottaminen on organisoitu ja vastuutettu.
Toimenpide 4.1	Määrittele, kuka/ketkä vastaavat tiedoksiantojen ja ilmoitusten tekemisestä sekä niissä tarvittavien tietojen keräämisestä.
Toimenpide 4.2	Määrittele, kenelle tiedotetaan: 1) Ennakollinen tiedotus, kun tunnistamistietojen käsittelyoikeuksia ollaan ottamassa käyttöön; a) yhteisötilaajan tietoverkon käyttäjät, b) yrityssalaisuuksia käsittelevät, c) tietosuojavaltuutettu. 2) Jälkikäteinen tiedotus, kun tunnistamistietoja on käsitelty manuaalisesti; a) viestintäverkon käyttäjät, joiden tunnistamistietoja on käsitelty manuaalisesti (tiedotettava myös niille käsittelyn kohteille, jotka eivät liittyneet epäiltyyn väärinkäytökseen) ja b) työntekijöiden edustajat sekä c) tietosuojavaltuutettu.
Toimenpide 4.3	Määrittele, mistä tiedotetaan: 1) Ennakollinen tiedotus; a) tunnistamistietojen käsittelyssä noudatettavien menettelyiden perusteet ja käytännöt, b) seikat ja perusteet, joiden perusteella automaattinen tai manuaalinen käsittely olisi mahdollista, c) tehtävät, joissa tunnistamistietoja voidaan käsitellä sekä d) YT-menettelyssä tehdyt päätökset. 2) Jälkikäteinen tiedotus käsittelyn kohteelle; a) tunnistamistietojen käsittelyn peruste, ajankohta ja kesto, b) syy, jonka vuoksi tunnistamistietojen käsittelyyn on ryhdytty, c) käsittelijät ja d) käsittelystä päättänyt henkilö. 3) Vuosittainen selvitys työntekijöiden edustajille ja tietosuojavaltuutetulle; a) tunnistamistietojen manuaalisten käsittelykertojen määrä ja perusteet.
Toimenpide 4.4	Suunnittele tiedottamisprosessi, kuinka tiedotetaan: 1) Ennakollinen tiedotus; a) varaa työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi (jos kuulut yhteistoimintavelvoitteen piiriin), b) tiedota työntekijöille valvonnan tarkoituksesta, käyttöönotosta

	ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä sekä c) harkitse, kuinka käyttöohjeet ja valvontamekanismit tuodaan käyttäjien tietoon. 2) Jälkikäteinen tiedotus käsittelyn kohteelle: a) Huolehdi, että kaikki käsittelyyn osallistuneet allekirjoittavat viestintäverkon käyttäjälle annettavan selvityksen. b) Lähetä laatimasi selvitys henkilölle/henkilöille, joiden tunnistamistietoja on käsitelty, kun se on mahdollista käsittelyn tarkoitusta vaarantamatta. c) Säilytä selvitys 2 vuotta. d) Laadi tallennettavista selvityksistä henkilötietolain (523/1999) 10 §:n mukainen rekisteriseloste, joka on kaikkien saatavilla. Vuosittainen selvitys työntekijöiden edustajille ja tietosuojavaltuutetulle tehdään ainoastaan silloin, kun tunnistamistietoja on käsitelty manuaalisesti kuluneen vuoden aikana.
Esimerkkejä hyvistä käytännöistä	Toimenpiteeseen 4.3 alakohtaan 2: Kaikesta havaitun väärinkäytöksen selvittämiseen liittyvästä toiminnasta, mukaan lukien tunnistamistietojen käsittely, pidetään tapahtumapäiväkirjaa, johon kirjataan toimenpiteet, ajankohdat, päätökset alla selvitys ja toimenpiteet osion toimenpide 3 mukaisesti. Vastuut kirjauksista on jaettu. Toimenpiteeseen 4.3 alakohtaan 2: Laadi mallipohjat tunnistamistietojen manuaalisesta käsittelystä annettavasta jälkikäteisestä selvityksestä. Yksityiskohtaisempaa tietoa annettavan selvityksen sisällöstä löytyy jäljempänä sivulla 16, selvitys ja toimenpiteet –osion alakohta B:ssä. Toimenpiteeseen 4.4. alakohtaan 1: Yhteisötilaaja voi valita tiedottamistavan. Kirjallinen tiedottaminen ehkäisee näyttöongelmia. Toimenpiteeseen 4.4 alakohtaan 2: Selvitys annetaan väärinkäytöksestä epäillylle tiedoksi henkilökohtaisesti poliisin tai asianmukaisen esimiehen toimesta (henkilöstöosaston edustajan läsnäolo organisaation sisäisten ohjeistusten mukaisesti). Niille tunnistamistietojen käsittelyn kohteille, jotka eivät tutkimusten mukaan liittyneet epäiltyyn väärinkäytökseen, voidaan tiedoksianto tehdä esimerkiksi sähköpostitse.
Huomioita	Tietosuojavaltuutetulle vuosittain annettavan selvityksen tekoaika lasketaan tietosuojavaltuutetulle toimitetusta ennakkoilmoituksesta tai edellisestä vuosi-ilmoituksesta. Vuoden aikana päättyneiden manuaalisten käsittelyjen lisäksi selvityksestä tulee käydä ilmi myös kyseisenä vuonna meneillään olevat, mahdollisesti jo aikaisemmin aloitetut tunnistamistietojen käsittelyt.
Apuvälineitä ja malleja	Tietosuojavaltuutetulle tehtävien ilmoitusten mallilomakkeet löytyvät osoitteesta http://www.tietosuoja.fi/46872.htm ja rekisteriseloste täyttöohjeineen osoitteesta http://www.tietosuoja.fi/2584.htm

Selvitys ja toimenpiteet

Kun havaittua yrityssalaisuuden luvatonta paljastamista ryhdytään selvittämään tai havaittuun tietoverkon poikkeamaan ryhdytään reagoimaan, on tunnistamistietojen käsittely vain yksi käytössä olevista keinoista. Selvitykseen osallistuvien tietohallinnon, turvallisuustoimintojen tai sisäisen tarkastuksen edustajien tulee ammattitaitoonsa nojaten arvioida tarve tunnistamistietojen käsittelylle yksittäistapauksessa ja huolehtia tunnistamistietojen asianmukaisesta käsittelystä organisaation määrittelemien käytäntöjen ja ohjeiden mukaisesti.

A. Havaittuasi poikkeaman tietoverkossa

1) arvioi poikkeaman mahdolliset vaikutukset tietoverkon ja sen laitteiden toiminnalle (tilanne-analyysi);
   a) miten laaja poikkeama on ja miten nopeasti se laajenee,
   b) mikä on sen vaikutus toimintaan ja mitä vahinkoja on aiheutunut tai todennäköisesti aiheutuu (esim. tietojen tai palvelujen saatavuus, tietojen luottamuksellisuus tai oikeellisuus, järjestelmän eheys, taloudelliset vahingot tai vahinkouhat, henkilövahingot),
2) jos poikkeama uhkaa verkon tai sen laitteiden tietoturvallisuutta ryhdy välittömiin toimiin uhan torjumiseksi tai sen vaikutusten rajoittamiseksi (kohdeosoitteiden sulkeminen; SVTSL 20 §);
3) arvioi onko kyseessä järjestelmästä aiheutuva vika vai inhimillinen toiminta;
4) jos poikkeama aiheutuu väärinkäytöksestä, harkitse jatketaanko selvittämistä;
5) harkitse, onko aihetta epäillä rikosta (täyttyykö rikoksen tunnusmerkistö) ja otetaanko yhteys poliisiin.

Selvitä toimeksiantosi rajat - mihin asti päätät toimenpiteistä itsenäisesti ja milloin konsultoit esimiestäsi.

Ota selvitykseen erikseen määritellyllä tavalla mukaan tarvittavat osallistujat organisaation eri yksiköistä.

B. Kun väärinkäytöstä ryhdytään selvittämään, määritä ja kirjaa

1) mitä tutkitaan (millaisesta poikkeamasta/häiriöstä on kyse; onko kyseessä epäilty maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvaton käyttö, yrityssalaisuuden paljastaminen tai muu vaaran aiheuttaminen tietojenkäsittelylle)
2) miten poikkeama/häiriö/mahdollinen väärinkäytös tai tietovuoto havaittiin:
   a) automaattinen hakutoiminto havaitsi poikkeaman viestinnässä,
   b) palvelun käyttökustannukset ovat nousseet epätavallisen korkeiksi,
   c) yrityssalaisuus on julkaistu tai sitä käytetään luvatta,
   d) viestintäverkossa havaittu sinne kuulumaton laite, ohjelma tai palvelu,
   e) muu näihin rinnastuva perusteltu seikka (yksilöi)
3) milloin ja missä tapahtunut
4) mihin järjestelmään tai tietoon poikkeama kohdistuu: arvioi ja kirjaa
   a) onko kyseessä keskeinen yrityssalaisuus; miten se on keskeinen (organisaation määrittämien kriteerien perusteella),

b) onko kyseessä lähdesuojan alainen tieto

5) kuka on vastuussa tästä järjestelmästä tai tiedosta
6) yksilöi järjestelmät, joiden tunnistamistietoja käsitellään (organisaation sähköposti, verkkosivut, sisäverkon palvelut, jokin muu)
7) kuka päättänyt tutkinnasta ja ketkä tunnistamistietoja käsittelevät sekä keneltä saa lisätietoja yllä esitetyistä havainnoista (yhteystiedot)
8) kenen tunnistamistietoja käsitellään; kerää tarvittaessa selvityksen kohteiden nimet erilliseen listaan.
9) milloin tutkinta aloitettiin ja milloin lopetettiin

Kysymyksiä ja vastauksia

Haittaohjelmat

Kysymys: Saako ylläpitäjä etsiä haittaohjelmien saastuttamia tietokoneita tietoliikennelokeista haittaohjelmalle tunnusomaisen liikennöinnin avulla?

Kysymys: Ulkopuolinen taho ilmoittaa yhteisötilaajan tietoverkon laitteen levittävän haittaohjelmaa. Saako kyseisen laitteen selvittää tietoliikenteen lokeista?

Vastaus: Molemmat ovat SVTSL:n 20 §:n sallimia tietoturvatoimenpiteitä.

Kysymys: Eräs käyttäjä saa toistuvasti haittaohjelmatartuntoja tietokoneelleen. Saako yhteisötilaaja selvittää tietoliikennelokeista, millä verkkosivuilla käyttäjä vierailee?

Vastaus: Mikäli ko. verkkosivuilla vierailu on kielletty käyttösäännöissä ja käyttäjää on tästä asianmukaisesti ohjeistettu, voidaan SVTSL:n 13 §:n nojalla selvittää, onko käyttäjä vieraillut kielletyillä sivuilla.

Tietojen kalastelu (Phishing)

Kysymys: Saako yhteisötilaaja suodattaa viestejä, joissa yritetään huijata käyttäjiä paljastamaan yhteisötilaajan tietoja ulkopuoliselle taholle?

Vastaus: Kyllä, SVTSL:n 20 §:n mukaisena tietoturvatoimenpiteenä.

Kysymys: Saako yhteisötilaaja selvittää, kuka käyttäjä vastaanotti viestin, jolla yritetään huijata käyttäjää paljastamaan yrityssalaisuuksia ulkopuoliselle taholle?

Vastaus: Jos viestissä yritettiin urkkia maksuvälinetietoja tai tietoja, joita voidaan käyttää yhteisötilaajan viestintäpalvelujen tietoturvan tai viestintämahdollisuuksien vaarantamiseen, viestin vastaanottajat saa tunnistamistietojen yleiset käsittelysäännöt huomioiden selvittää SVTSL:n 20 §:n nojalla. Jos viestissä yritettiin urkkia yhteisötilaajan yrityssalaisuuksia, viestin vastaanottajat saa muussa, kuin edellä esitetyssä tapauksessa selvittää SVTSL:n 13 §:n nojalla.

Kysymys: Saako yhteisötilaaja selvittää viestinnän lokeista käyttäjät, jotka vastasivat huijausviestiin ja sulkea heidän tunnuksensa asian tutkimisen ajaksi?

Vastaus: Jos viestinnässä yritettiin urkkia tietoja, joita voidaan käyttää yhteisötilaajan viestintäpalvelujen tietoturvan tai viestintämahdollisuuksien vaarantamiseen, voi yhteisötilaaja ryhtyä SVTSL:n 20 §:n nojalla perusteltuihin turvaamistoimenpiteisiin. Mikäli tietojen kalasteluviesti on sisällöltään muunlainen, tapahtuu selvittäminen SVTSL:n 13 §:n nojalla.

Häiriköinti ulkoisissa palveluissa

Kysymys: Saako yhteisötilaaja selvittää, kuka käyttäjä on häiriköinyt kolmannen osapuolen verkkopalvelussa?

Vastaus: Käyttäjien väärinkäytöksiä ulkoisissa palveluissa voidaan selvittää SVTSL:n 13 a §:n mukaisesti, kun toiminta on selvästi vastoin asianmukaisesti laadittua käyttäjien ohjeistusta. Kolmannen osapuolen verkkopalvelussa häiriköivä käyttäjä voidaan tunnistaa tietyissä tilanteissa myös SVTSL:n 20 §:n mukaisin oikeuksin viestintäviraston kannanotossa 268/64/2010 linjatuin reunaehdoin (kts. liite 1).

> Viestintäviraston arvion mukaan muiden käyttäjien viestintäpalvelun käyttömahdollisuuksia merkittävästi ja välittömästi rajoittavan käyttäjän toimia voidaan pitää sähköisen viestinnän tietosuojalaissa tarkoitettuna tietoturvatoimenpiteisiin ryhtymiseen oikeuttavana viestintäpalvelulle haittaa aiheuttavana häiriönä. Tietoturvatoimenpiteisiin ryhtymistä voidaan pitää perusteltuina myös viestintäpalvelun muiden käyttäjien viestintämahdollisuuksien turvaamiseksi.
> Arvioitaessa käyttömahdollisuuksien rajoittumisen merkittävyyttä, on huomiota kiinnitettävä ainakin siihen, että toimilla saavutettavan hyödyn on oltava olennaisesti luottamuksellisen viestin suojalle aiheutuvaa haittaa suurempi. Arvioinnissa on syytä kiinnittää huomiota ainakin kohteena olevan palvelun merkittävyyteen sekä mahdollisten rajoitustoimien todennäköisyyteen ja vaikuttavuuteen käyttäjien keskuudessa.
> Arvioitaessa käyttömahdollisuuksien rajoittumisen välittömyyttä, on huomiota kiinnitettävä rajoitustoimenpiteiden toteutumisen todennäköisyyteen. Välittömyyden arviointi perustuu tyypillisesti käsittelytarvetta arvioivan toimijan omaan kokemukseen rajoitustoimenpiteiden todennäköisyydestä. Jo aloitettujen rajoitustoimenpiteiden osalta ei välittömyysarviointia tarvitse tehdä. Viestintäviraston tulkinnan mukaan kolmannen osapuolen palvelussa häiriköivät käyttäjät voidaan tunnistaa tunnistamistietoja käsittelemällä yllä kuvatut reunaehdot huomioiden. Tunnistamistietojen käsittelyn edellytyksenä on kuitenkin aina se, että käsittelyn tavoitetta ei voida saavuttaa millään muulla tavoin. Viestintämahdollisuuksien rajoittamista lievempänä toimenpiteenä käyttäjä voidaan vain tunnistaa yhteydenottoa varten.

Roskaposti

Kysymys: Saako yhteisötilaaja suodattaa roskapostia?

Vastaus: Saa. (SVTSL 20 §)

Kysymys: Saako yhteisötilaaja selvittää roskapostia lähettävän käyttäjän tietoverkostaan?

Vastaus: Kun roskapostin lähettäminen on kielletty yhteisötilaajan käyttösäännöissä, voidaan kiellon noudattamista valvoa SVTSL:n 13 a §:n mukaisesti. Jos lähetetyn roskapostin suuri määrä merkittävästi heikentää viestintäpalvelun käyttöä, niin käyttäjän saa selvittää myös tietoverkon tietoturvasta huolehtimiseksi (SVTSL 20 §).

Kysymys: Saako yhteisötilaaja selvittää ja eristää roskapostia lähettävän, oletettavasti haittaohjelman saastuttaman tietokoneen tietoverkostaan?

Vastaus: Saa. (SVTSL 20 §)

Käyttäjien asentamat palvelut

Kysymys: Saako yhteisötilaaja etsiä tietoverkostaan ohjeiden vastaisesti pystytettyjä palveluita, kuten tiedosto- ja WWW-palvelimia, P2P-trackereita tai langattomia tukiasemia, tietoliikenteen tunnistamistietojen avulla?

Vastaus: Jos palvelut häiritsevät muita tietoverkon laitteita tai haittaavat merkittävästi tietoverkon viestintäpalvelujen käyttöä tai muuten selkeästi vaarantavat tietoverkon tietoturvallisuuden, niitä saa selvittää SVTSL:n 20 §:n mukaisesti tietoturvatoimenpiteenä. Muuten kyseessä on ohjeiden vastaisen toiminnan selvittämistä SVTSL:n 13 §:n mukaisesti.

Kysymys: Entäpä jos kyseessä on luvaton sähköpostipalvelin?

Vastaus: Käyttäjien asentamien sähköpostipalvelimien yhteisölle haitallinen toiminta pitäisi voida estää tietoverkon palomuurein (outbound SMTP), jolloin itse palvelinten jäljittäminen on SVTSL:n 13 §:n mukaista ohjeiden vastaisen toiminnan selvittämistä.

Muut kysymykset

Kysymys: Saako ylläpito tarkkailla viestintäverkon liikennemääriä (ns. Flow-dataa) häiriöiden ja poikkeamien havaitsemiseksi?

Vastaus: Saa SVTSL:n 12 a §:n nojalla tilastollisena analyysina, josta ei voida tunnistaa yksittäistä käyttäjää.

Kysymys: Saako ylläpito tutkia käyttäjän tietokoneen tiedostoja, kirjautumistietoja tai kirjanmerkkejä väärinkäytösten selvittämiseksi?

Vastaus: SVTSL:n 13 § käsittelee vain viestinnän tunnistamistietojen käsittelyä. Tietojärjestelmien sisäiset mekanismit, kuten esimerkiksi kirjautumiset ja tietojärjestelmän käytön lokitiedot eivät kuulu SVTSL:n 13 a-k §:ien piiriin. Verkkoselailun historiatiedot ovat kuitenkin SVTSL:n mukaisia tunnistamistietoja.

Kysymys: Automaattisen haun kriteerit ovat liian suppeat! Eikö epäonnistuneita kirjautumisyrityksiä saa valvoa?

Vastaus: Yhteisötilaaja on käyttäjän ja yhteisön tietojärjestelmien välisessä viestinnässä viestinnän toinen osapuoli ja oikeutettu SVTSL 8 §:n nojalla käsittelemään tunnistamistietoja.

Kysymys: Voiko yhteisötilaaja siirtää sopimuksella SVTSL:n mukaiset velvoitteet ja vastuut tietoliikennepalveluiden tarjoajalle ts. ulkoistaa valvonnan avaimet käteen-periaatteella?

Vastaus: Yhteisötilaaja vastaa aina toiminnastaan, mutta voi pääsääntöisesti sopimuksin ulkoistaa toimenpiteet, joita on itse oikeutettu harjoittamaan.